Claims

The claimed invention is:

1. A method of identifying threats to a computing system received from a network, the computing system having a plurality of monitor modules including a first monitor module, comprising:

evaluating a message received from the network with the plurality of monitor modules;

identifying the message as a threat by one or more monitor modules;

receiving event data from the one or more monitor modules, the event data related to the message;

storing the event data in a first event record in a database on the computing system, the database including a plurality of second event records containing event data related to previous messages;

analyzing, after receipt of event data from any one of the plurality of monitor modules, the first event record and second event records in the database; and

transmitting a command to the first monitor module, in response to results of the analysis, the command including at least some event data from the first event record and a security action to be taken by the first monitor module.

2. The method of claim 1, wherein the event data includes information identifying the message, the type of threat potentially posed by the message, and an indication of a relative priority for the message.

3. The method of claim 1, wherein the action to be taken by the first monitor module is to block all future messages identified by the event data included in the command.

4. The method of claim 1, wherein analyzing comprises:

identifying the second event records that relate to the first event record; and

calculating a relative threat level for the message based on the second event records that relate to the first event record.

5. The method of claim 4, wherein determining comprises:

performing a Bayesian analysis on the first event record and the identified second event records to estimate the relative threat level of the message.

6. The method of claim 1 further comprising:

deleting from the database second event records that are older than a specified age.

7. The method of claim 4, wherein transmitting a command comprises:

determining, based on the calculated threat level, the security action necessary to protect the computing system from the message and the first monitor module necessary to perform the security action;

retrieving interface requirements for the first monitor module;

generating the command based on the event data, the interface requirements for the first monitor module, and the security action.

8. The method of claim 1, wherein the security action is a security action that the first monitor module did not perform based on the monitor module's internal evaluation of the message

9. A method of monitoring communication traffic on a network comprising:

evaluating, by a first computing system, a first message received from the network;

evaluating, by a second computing system, the first message received from the network

generating, by the first computing system, new event data related to the first message including a site priority determined by the first computing system;

transmitting the new event data to a security facility;

storing the new event data at the security facility in an event database that includes pre-existing event data;

calculating, at the security facility and based on the event data in the event database, a network threat level for the message; and

issuing commands based on the network threat level from the security facility to the second computing system.

10. The method of claim 9, wherein the first computing system is a plurality of first computing systems.

11. The method of claim 10, wherein the second computing system is a plurality of second computing systems.

12. The method of claim 9, wherein the commands include at least some of the new event data identifying messages for the second computing system to act on and an action to be performed on the identified messages.

13. The method of claim 9 further comprising:

deleting from the event database pre-existing event data that are older than a specified age.

14. The method of claim 9, wherein the calculating operation is repeated after each receipt of new event data from one of the plurality of computing systems.

15. The method of claim 14, wherein calculating further comprises:

identifying pre-existing event data that relate to the new event data; and

determining if the identified pre-existing event data indicate that the threat posed by the message is greater or lesser than a predetermined threshold.

16. The method of claim 15, wherein determining comprises:

performing a Bayesian analysis on the event data that relate to the new event data to estimate the network threat level of messages related to the new event data.

17. A method for deleting messages received by a computing system from a network comprising:

receiving a message in a buffer on the computing system, the message directed to a destination on the computing system;

evaluating the message with a plurality of monitor modules;

if the message is identified as a potential threat by one or more of the monitor modules,

storing the output of the monitor modules related to the message in a new event record in a database containing a plurality of previous event records, the output including event data describing attributes of the message, a threat type, and an assigned priority;

analyzing event records in the database;

selectively deleting the message from the buffer before delivery to the destination.

18. The method of claim 17 further comprising:

deleting from the database previous event records that are older than a specified age.

19. The method of claim 17, wherein the determining operation is repeated each time a new event record is received.

20. The method of claim 19, wherein determining further comprises:

identifying all event records in the database that relate to the new event record;

performing a Bayesian analysis on the event data in the identified event records; and

estimating a threat level for the message based on the results of the Bayesian analysis.

21. The method of claim 17, further comprising:

transmitting a command to a security device to automatically delete future messages in the buffer having specified event data for a specified period of time.

22. The method of claim 17, further comprising:

transmitting a command to a security device to automatically delete future messages in the buffer sent to a specified computer port for a specified period of time.

23. The method of claim 17, wherein the event data includes an event type, an event description, an event date and time, at least one indication of the source of the message, and at least one indication of the destination of the message.

24. A computer readable medium comprising:

a database of event records for each message received within a period of time by a computing system and identified as a threat by one or more monitor modules on the computing system, each event record including event data provided by the one or more monitor modules that identified the message as a threat, the event data including

a priority level of the message assigned by one or more monitor modules,

an event identifier,

an event type,

an event description,

an event priority,

a date and time associated with the message,

data identifying the message's source, and

data identifying the message's destination.

25. The database of claim 24, wherein the event data identifying the message's source comprises:

a source IP address of the message;

a source port of the message;

a source URL for the message; and

a designation indicating if the message is from a source internal to the computing system.

26. The database of claim 24, wherein the event data identifying the message's destination comprises:

a destination IP address of the message;

a destination port of the message;

a destination URL for the message; and

a designation indicating if the message is to a destination internal to the computing system.

27. The database of claim 24, wherein the event data includes data identifying the computing system that received the message.

28. The database of claim 27, wherein the event data includes data identifying any actions taken by monitor modules on the computing system upon receipt of the message.

29. The database of claim 24, wherein the event data is provided in disparate forms by the monitor modules and stored in a standardized form in the event record.